UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/584,118	04/27/2007	Shunichi Oshima	IXIO127677	9860

26389   7590   10/30/2009
CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER
DESIR, PIERRE LOUIS

ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
10/30/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 April 2007*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 April 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the
> subject matter which the applicant regards as his invention.

2.   Claim 4 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for

failing to particularly point out and distinctly claim the subject matter which applicant regards as

the invention.

Claim 4 recites the limitation "the data" in the last line of the claim. There is insufficient

antecedent basis for this limitation in the claim.

Note: The claim is not specific as to whether the data that is to be sent is data that is

generated from the biometric information or other data that is generated to sent after user

authentication.

Claim Objections

3.   Claim 1 is objected to because of the following informalities: "network

connection function" should be "network connection means". Appropriate correction is

required.

It should be noted that by disclosing "network communication means", it is implied that

the device contains "network connection function." Therefore, the above objection may be

resolved by either replacing "function" with means or "means" with "function."

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

5.   Claims 1-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Socolofsky, US 20030214779 A1 in view of Poo et al. (Poo), US 20030005336 A1.

Regarding claim 1, Socolofsky discloses a portable server device (i.e., portable network

server) (see paragraph 18) comprising a local server for processing data between itself an a

communication terminal equipped with a network connection means (i.e., using the portable

network server, a local area network is created for accessing the sever. The 2-node network uses

a universal serial bus Ethernet adapter to connect a PC to the portable server using a cross-over

Ethernet cable. A user can then configure the server (see fig. 7 and paragraph 37). Thus, the PC

(i.e., communication terminal is equipped with a network connection function. And, since

connection between the PC and the server is achieved through USB adapter, both the PC and the

server contain network connection function. Therefore, the Portable network server contains a

local server since it can communicate with PC); a network server for processing data between

itself and a network connected to the communication terminal by said communication terminal's

network connection function (i.e., a portable network server to share multimedia content over a

home network and over the Internet. the home network is a local area Ethernet network

implementing the TCP/IP network protocol. The server and a browser enabled PC are connected

to each other on the home network via a home router or gateway. Internet connectivity is

provided via a DSL modem, cable modem, or other communication device, which is connected

to the home router or gateway. Using the browser enabled PC residing on the home router or

gateway, a user can remotely create and administer a personalized website that is hosted on the

server (i.e., the portable server having a network server for processing data between itself and a

network (i.e., Internet) connected to the PC). The user can publish multimedia content to the

website from the PC and display multimedia stored on the server using the PC) (see fig. 8,

paragraph 38).

Socolofsky does disclose the server includes an operating system (i.e., a control) which

includes one or more programs that control the operating of the computer and manage the

allocation of resources (see paragraph 34), wherein permission (i.e., use of the network and

server) may be granted or denied to users (see paragraph 38).

Socolofsky, however, does not specifically disclose that the portable server comprises an

individual authenticator for authenticating an individual based on biometric information; and a

control that makes said local server and said network useable only when authenticated by said

individual authenticator.

However, Poo discloses a portable device which includes a microprocessor, a non-

volatile memory coupled thereto, and a biometrics-based authentication module controlled by the

microprocessor. Preferably, the biometrics technology used is fingerprint authentication

technology, and flash memory is used as the non-volatile memory. The fingerprint authentication

module automatically prompts the user to register his/her fingerprint with the portable device

upon its first use. A compact and encrypted version of the fingerprint is stored in the portable

device's flash memory when the registration process is completed. Upon a subsequent use, the

fingerprint authentication module reads the user's fingerprint, compares it with the registered

fingerprint stored in the flash memory and reliably determines whether there is a match between

the two. If a match is identified, authentication of the user's identity is successful, and the

authenticated user is granted access to the restricted resource (see paragraph 7).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the

invention to have combined the teachings described by Poo with the teachings described by

Socolofsky to arrive at the claimed invention. A motivation for doing would have been to

provide a secured access control mechanism for protection against unauthorized access.

Regarding claim 2, Socolofsky discloses a personal server as described above (see claim

1 rejection).

Socolofsky, however, does not specifically disclose a personal server wherein said

individual authenticator is equipped with a biometric information recognition device and

authenticates an individual according to whether or not biometric information read by the

biometric information recognition device matches registered biometric information that was

previously registered.

However, Poo discloses a portable device which includes a microprocessor, a non-

volatile memory coupled thereto, and a biometrics-based authentication module controlled by the

microprocessor. Preferably, the biometrics technology used is fingerprint authentication

technology, and flash memory is used as the non-volatile memory. The fingerprint authentication

module automatically prompts the user to register his/her fingerprint with the portable device

upon its first use. A compact and encrypted version of the fingerprint is stored in the portable

device's flash memory when the registration process is completed. Upon a subsequent use, the

fingerprint authentication module reads the user's fingerprint, compares it with the registered

fingerprint stored in the flash memory and reliably determines whether there is a match between

the two. If a match is identified, authentication of the user's identity is successful, and the

authenticated user is granted access to the restricted resource (see paragraph 7).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the

invention to have combined the teachings described by Poo with the teachings described by

Socolofsky to arrive at the claimed invention. A motivation for doing would have been to

provide a secured access control mechanism for protection against unauthorized access.

Regarding claim 3, Socolofsky disclose a portable server as described above (see claim 2

rejection).

Socolofsky does not specifically disclose a portable server further comprising a data

encryptor for encrypting stored data using said read biometric information.

However, Poo discloses a portable device wherein templates are generated according to

the fingerprint module, wherein the templates generated are encrypted (see paragraphs 23, 31,

49-51).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the

invention to have combined the teachings described by Poo with the teachings described by

Socolofsky to arrive at the claimed invention in order to provide added security against hacking

(see paragraph 23).

6.   Claims 5-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Socolofsky and Poo, further in view of Makela et al. (Makela), US 20030157959 A1.

The combination of Socolofsky and Poo disclose a portable server as described above (see claim 1 rejection).

Although Socolofsky disclose a portable server further comprising a communication cable (see paragraph 37), the combination, however, does not specifically disclose a portable server receiving power from said communication terminal via said communication cable.

However, Makela discloses a portable server that uses an optional USB plug connection between itself and a personal computer to be provided data and power (see claim 34).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Makela with the teachings described by Socolofsky and Poo to arrive at the claimed invention. A motivation for doing so would have been to provide the portable server with the added functionality to be powered in places wherein AC/DC is not available.

Regarding claim 6, Socolofsky discloses a portable server device (see claim 5 rejection) wherein said communication cable is USB (see paragraph 37).

7.   Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Socolofsky and Poo, further in view of Brandys, US 20020186838 A1.

The combination of Socolofsky with Poo discloses a device as described (see claim 2 rejection).

The combination, however, does not specifically disclose a device further comprising a communication encryptor that, when said read biometric information matches said registered biometric information, generates and retains a key used in a public key encryption system based on said read biometric information, and encrypts the data to be sent using the key.

However, Brandys discloses a device wherein in response to authenticating biometric information that is provided by a user, a public key is generated and retain to encrypt incoming messages (see abstract, paragraph 15 and 24).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Brandys with the teachings described by Socolofsky and Poo to arrive at the claimed invention. A motivation for doing so would have been to authenticate messages.

Conclusion

8.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to PIERRE-LOUIS DESIR whose telephone number is (571)272-7799. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dwayne Bost can be reached on (571)272-7023. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available

through Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the

Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from

a USPTO Customer Service Representative or access to the automated information system, call

800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/PIERRE-LOUIS DESIR/
Examiner, Art Unit 2617